UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
SUBJECT PREMISES and USER

Case No. 3:23-mj-05303

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
Subject Premises and User as further described in Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252A(a)(1),(a)(2), (a)(5)(B), (b), (g) 2251(d), (d)	Possession, Transportation, Receipt, Distribution, Access with Intent to View, Advertising of Child Pornography, Engaging in Child Exploitation Enterpris, and attempt/conspiracy

The application is based on these facts:

✓ See Affidavit, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

DAVID BACKLUND
Digitally signed by DAVID BACKLUND
DN: c=US, o=U.S. Government, ou=Dept of Justice, ou=FBI, cn=DAVID BACKLUND
0.9.2342.19200300.100.1.1=15001004058341
Date: 2023.08.09 16:44:49 -04'00'

Applicant's signature

David J. Backlund, Special Agent
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/11/2023

Judge's signature

City and state: Tacoma, Washington

David W. Christel, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
PIERCE COUNTY)

I, David J. Backlund, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since September 2008. I was previously employed as a Special Agent with the Air Force Office of Special Investigations for eight years and nine months. As part of my duties as an FBI Special Agent, I am assigned to investigate violations of federal law, including the online exploitation of children. This includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the detection and investigation of criminal offenses. I have written, executed, and/or participated in the execution of numerous search warrants. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained expertise in these investigations through training, discussions with other law enforcement officers, and everyday work related to conducting these types of investigations. I have viewed numerous images and videos depicting the sexual exploitation of children in a variety of media, both in the course of my professional training and in the investigation of criminal offenses. I have also spent significant time interacting with and observing children as part of my professional duties and in my personal experience. I have investigated numerous cases involving child victims. All age estimations in this affidavit

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

are based on, among other things, my training and experience as a criminal investigator who specializes in offenses involving children, as well as my personal life experience.[1]

PURPOSE OF THE AFFIDAVIT

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the property located at 310 NE Kissin Tree Lane, Tahuya, Washington 98588 (hereinafter referred to as the "SUBJECT PREMISES"), located in Mason County in the Western District of Washington and the person of Joseph Martin (the SUBJECT USER) more fully described in Attachment A, for the items described in Attachment B, both of which are attached and incorporated herein by reference.

3. There is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(1), (a)(2), (a)(5)(B), (b)(1), (b)(2), and (g) (transportation, distribution, receipt, possession, and access with intent to view child pornography, conspiracies and attempts to commit such offenses, and engaging in a child exploitation enterprise) and 18 U.S.C. § 2251(d) and (e) (advertising child pornography and conspiracy and attempt to advertise child pornography) (hereinafter referred to as the "TARGET OFFENSES") have occurred and that the evidence, fruits, contraband and instrumentalities of those violations are located at the SUBJECT PREMISES.

4. The statements contained in this affidavit are based in part on information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents and agencies; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent

[1] As used in this affidavit, the term "child pornography" refers to any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(8)(a).

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

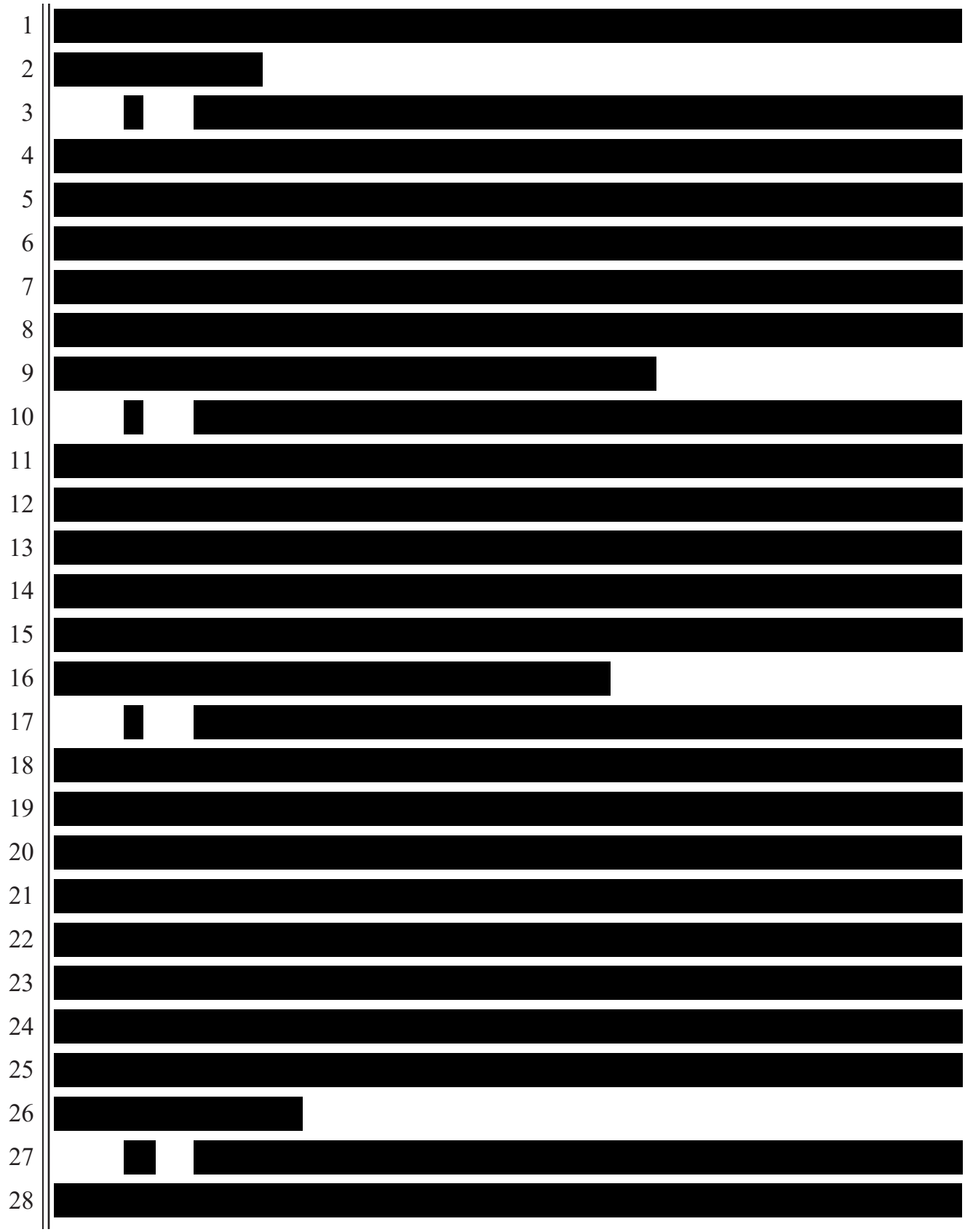
investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

5. The investigation, described more fully below, involves a website (hereinafter referred to as the "TARGET WEBSITE") that facilitated the advertisement and distribution of child pornography [redacted] For the reasons set forth below, there is probable cause to believe that a particular user of the TARGET WEBSITE (hereinafter referred to as the "SUBJECT USER") who resides at the SUBJECT PREMISES in the Western District of Washington was a high-ranking administrator of the TARGET WEBSITE, has knowingly accessed and trafficked in child pornography over the TARGET WEBSITE, and that evidence, contraband, fruits, and instrumentalities of violations of the federal statutes listed above will be found at the SUBJECT PREMISES.

[redacted]

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

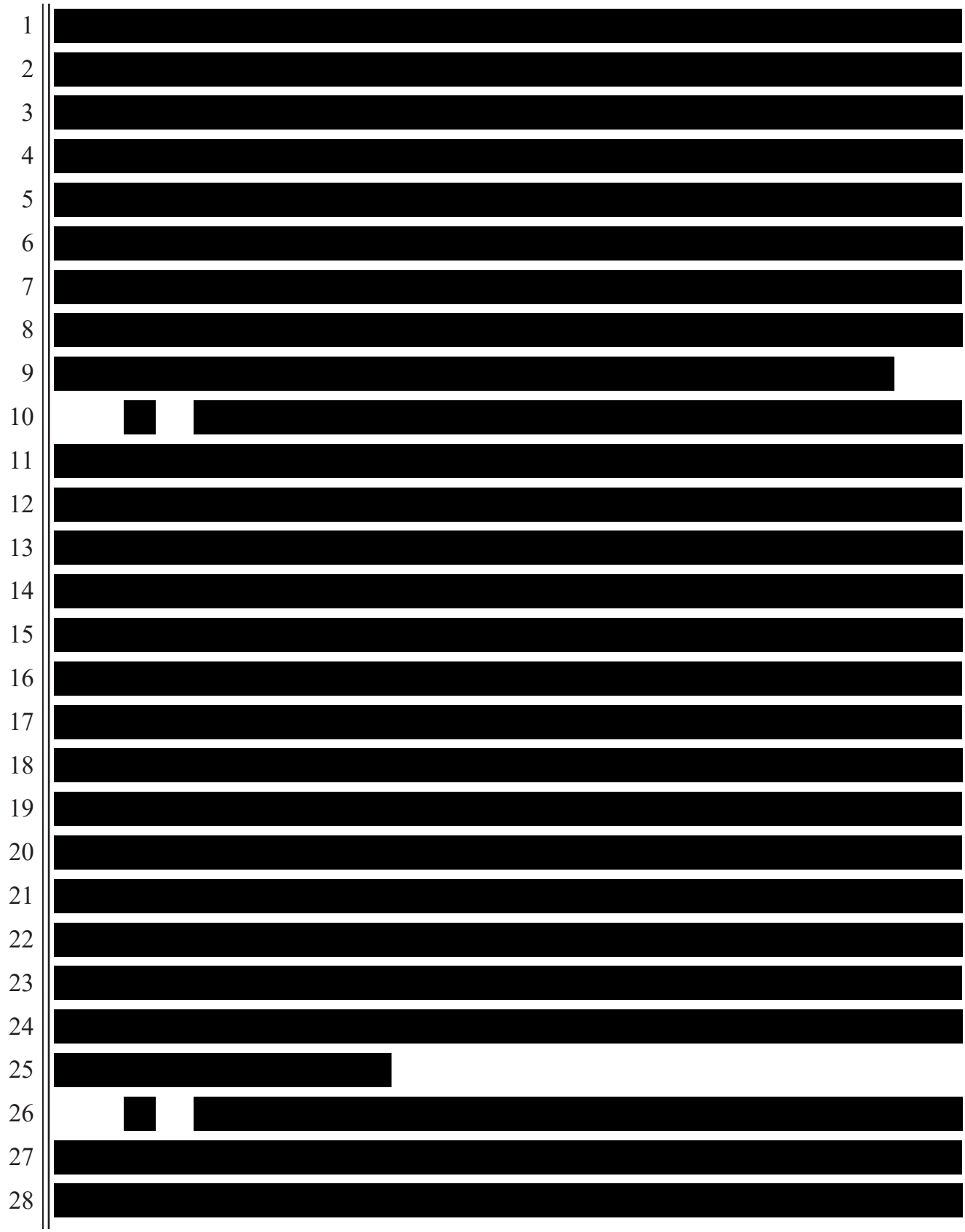
BACKGROUND TO THE INVESTIGATION

14. The requested search warrant is in furtherance of an investigation into the TARGET WEBSITE, which [redacted] facilitated the advertisement, distribution, and trafficking of child pornography. As set forth below, there is evidence that the SUBJECT USER, who resides at the SUBJECT PREMISES in the Western District of Washington, was a high-ranking administrator on the TARGET WEBSITE, knowingly trafficked in child pornography over the website, and continued to access the website until at least [redacted].

Description of the TARGET WEBSITE

[redacted]

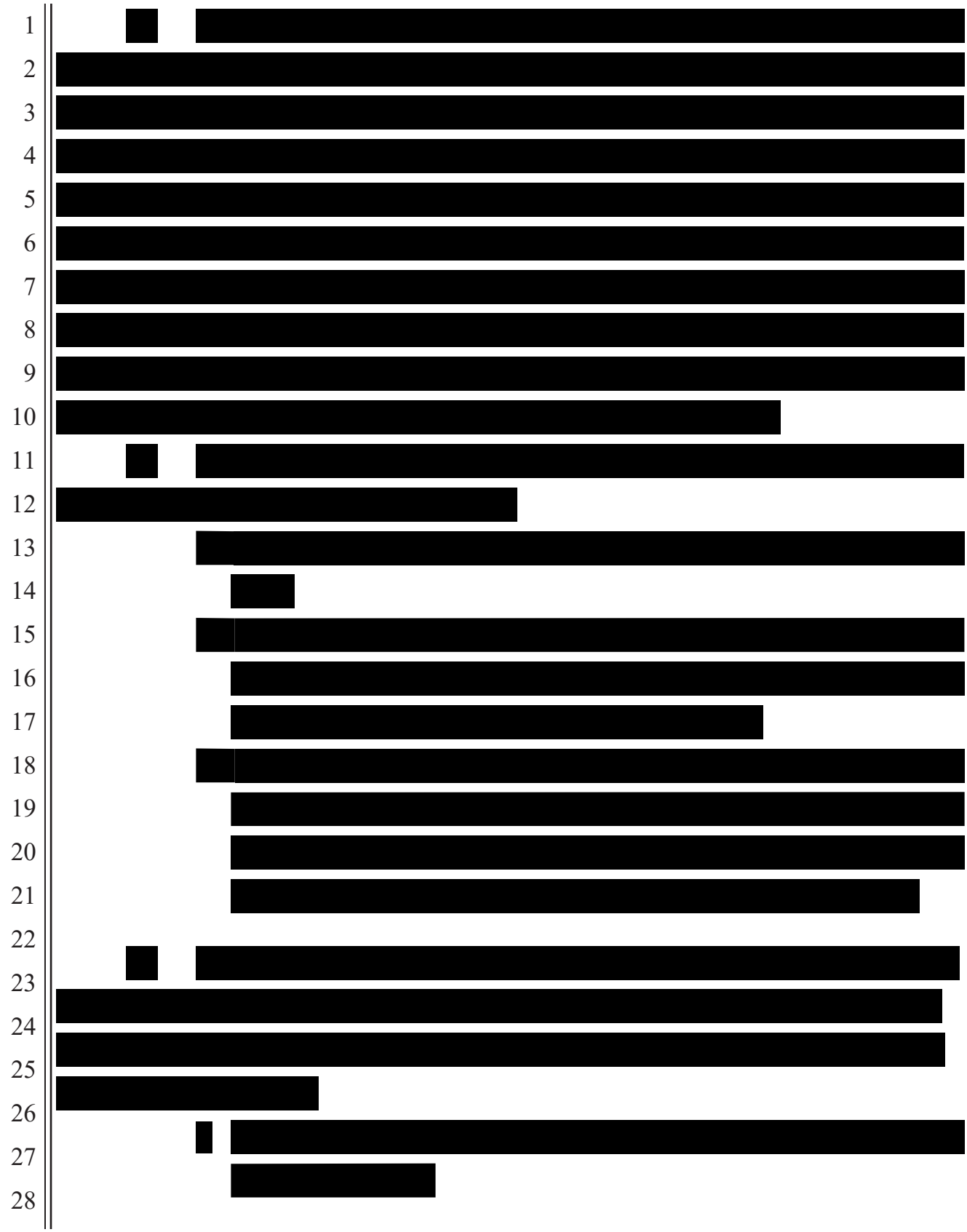
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



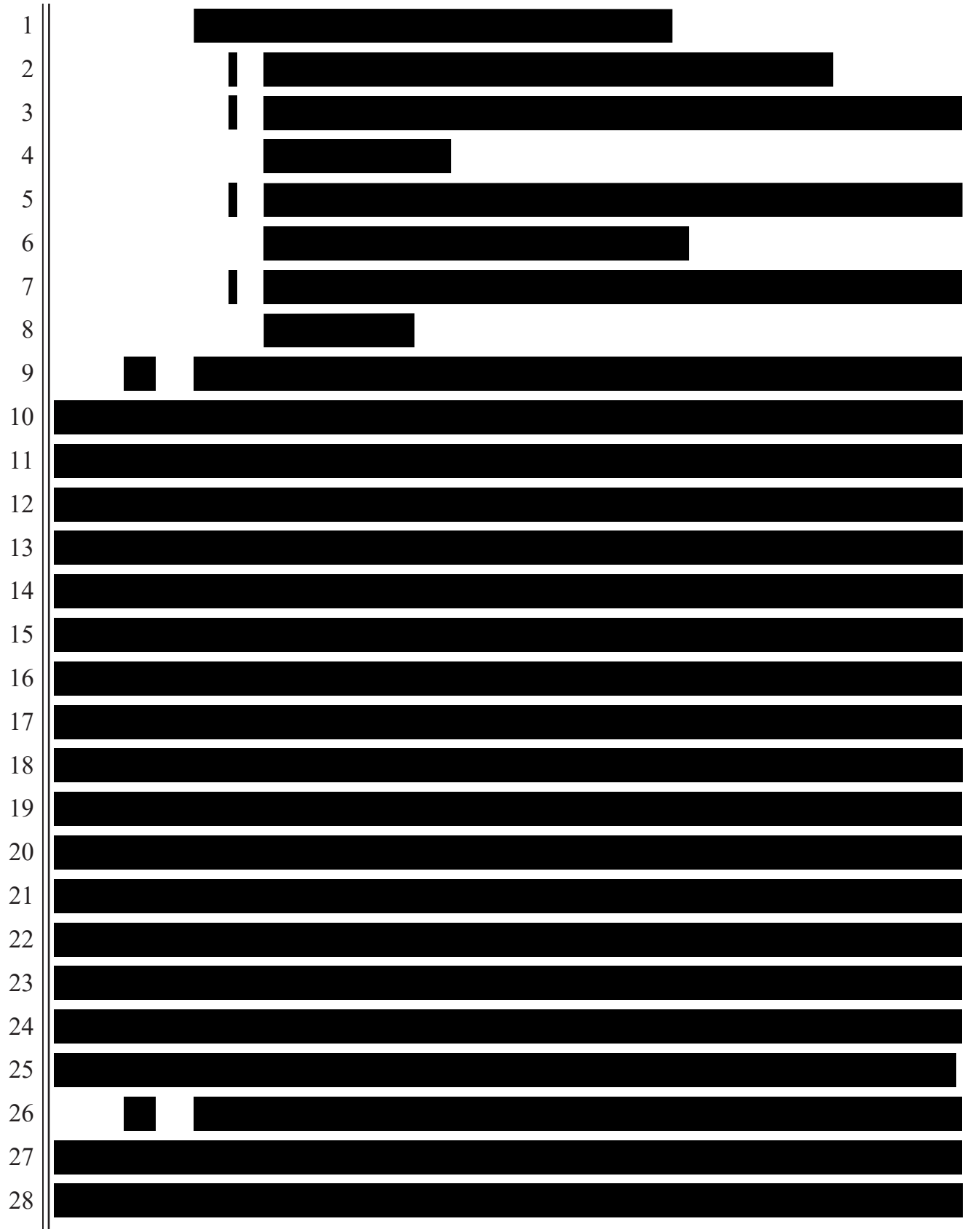
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

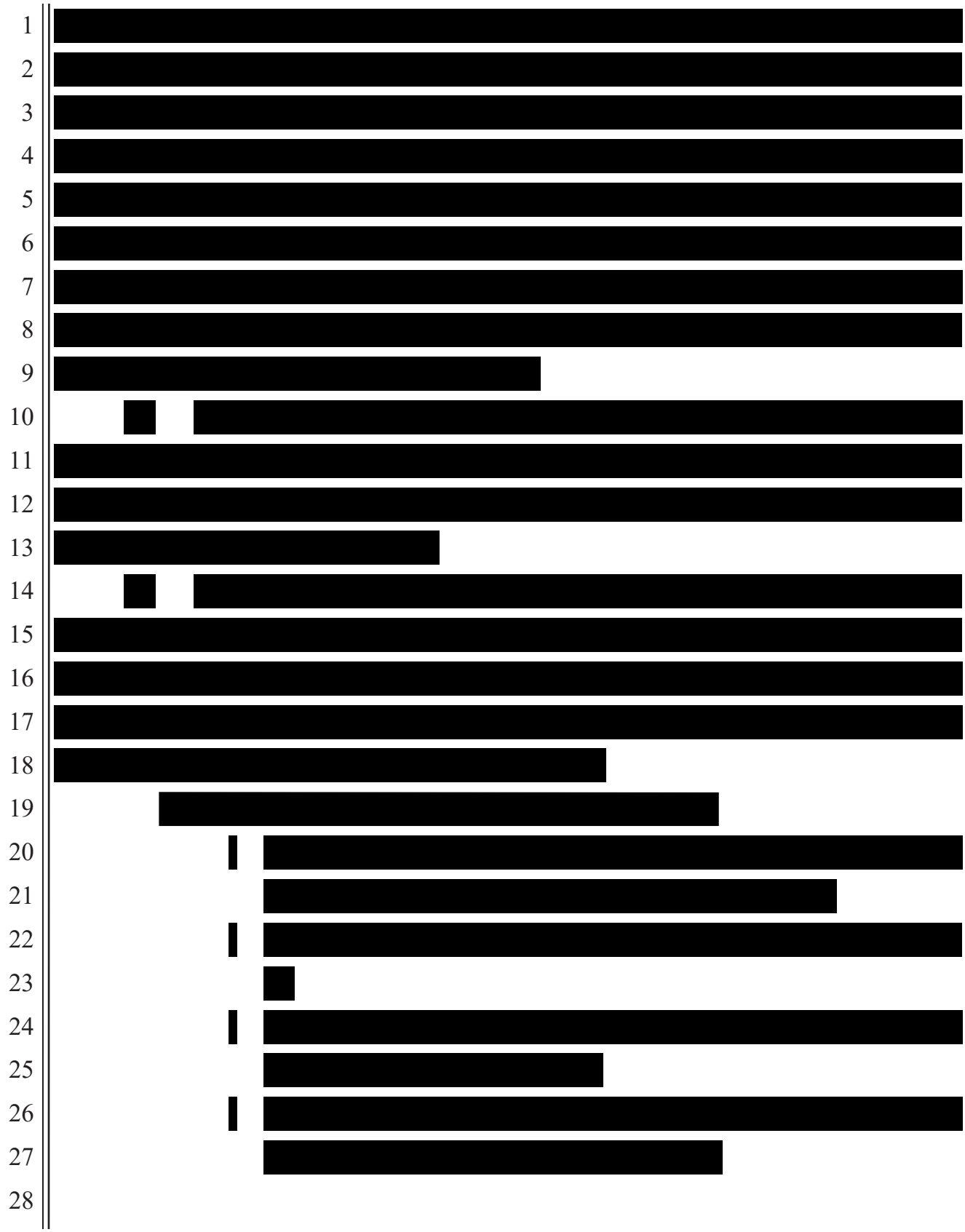
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



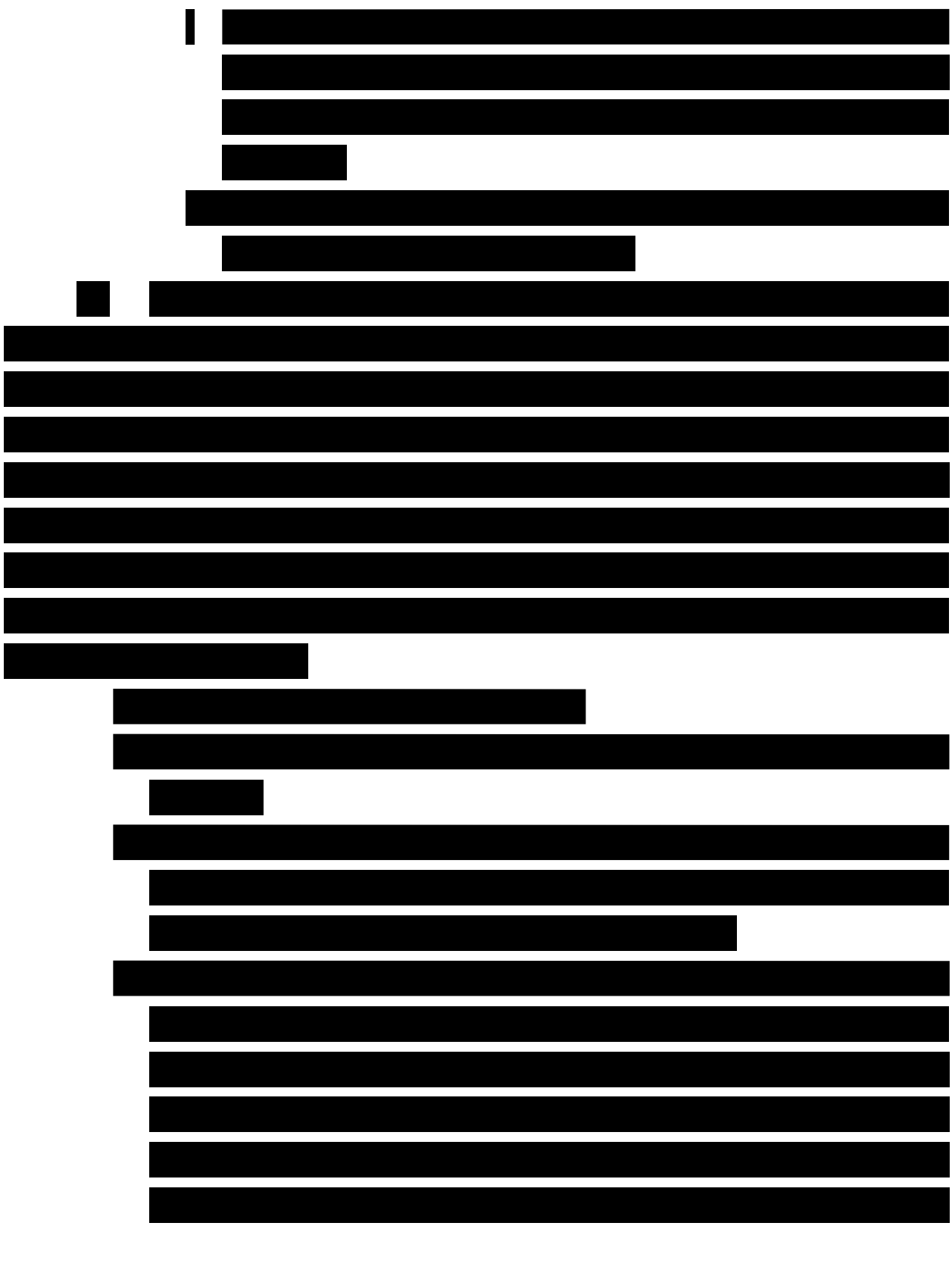
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



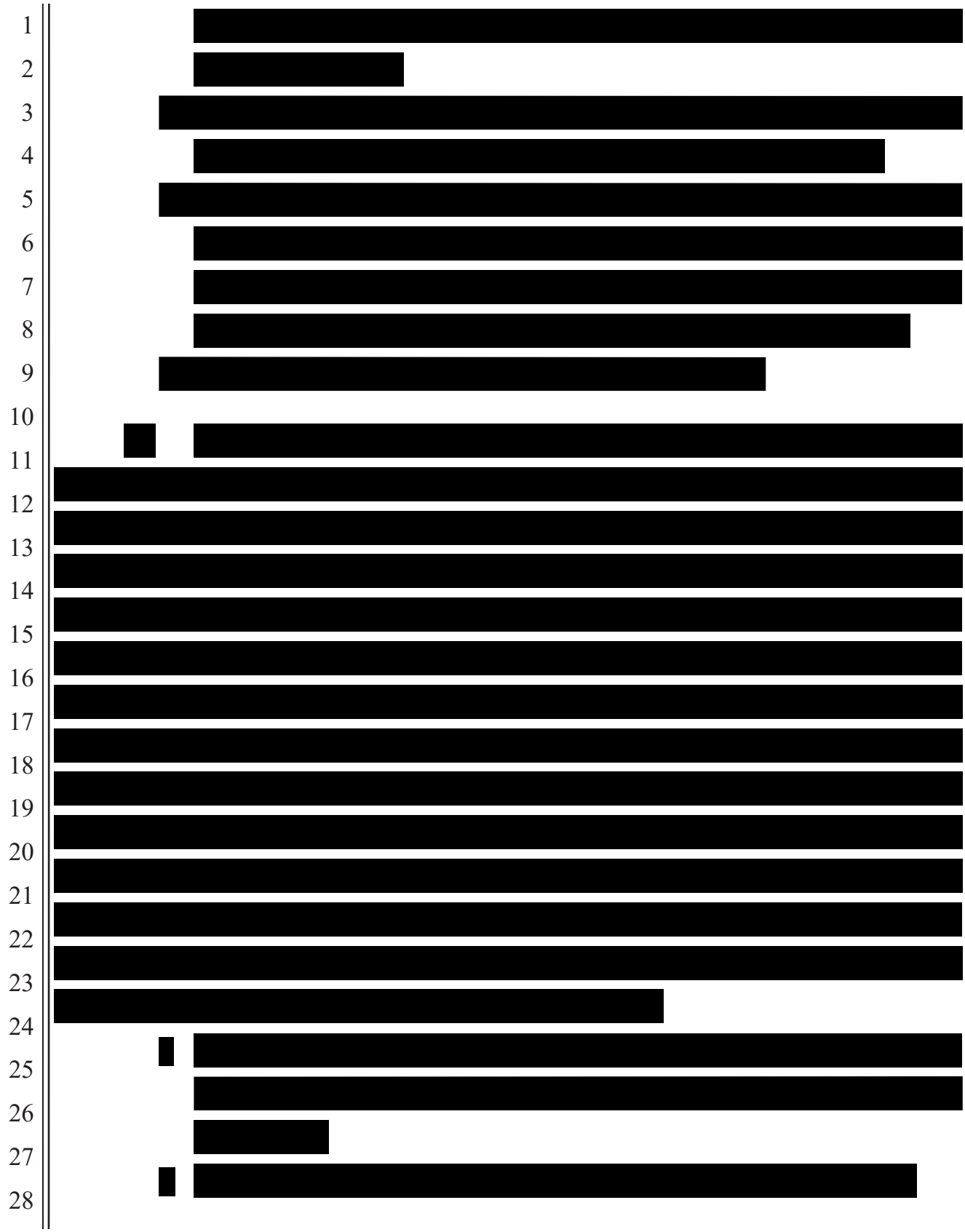
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



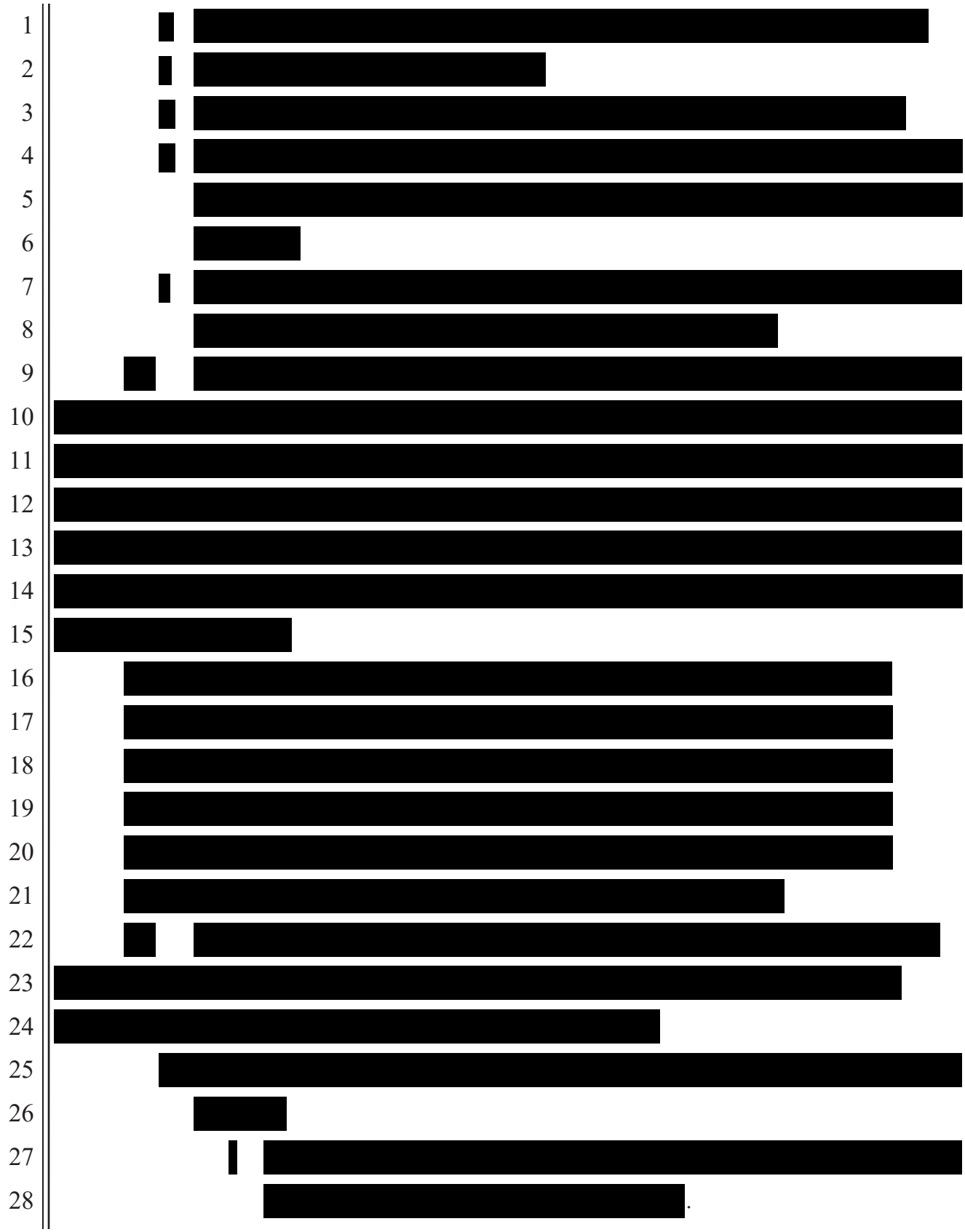
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

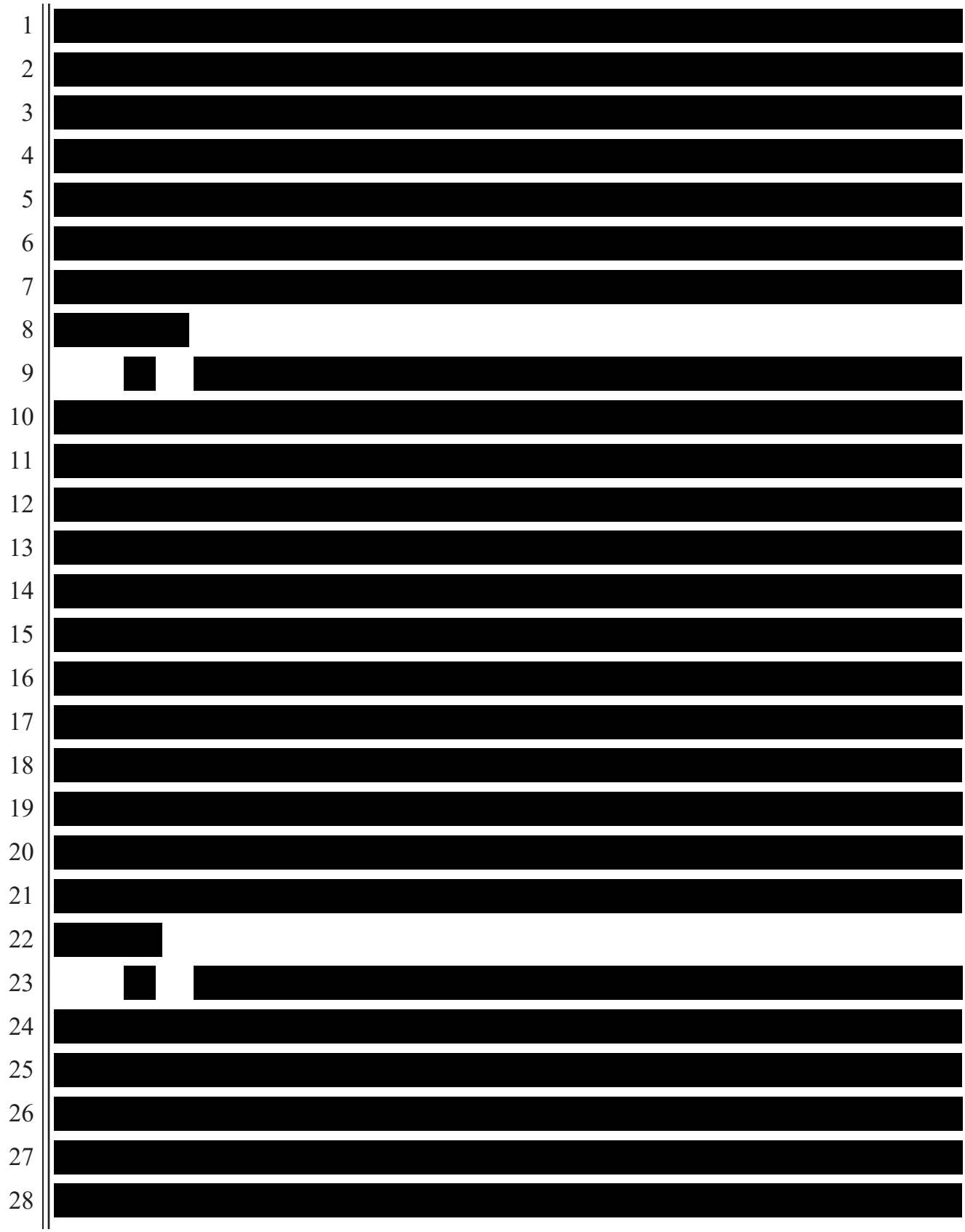


UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

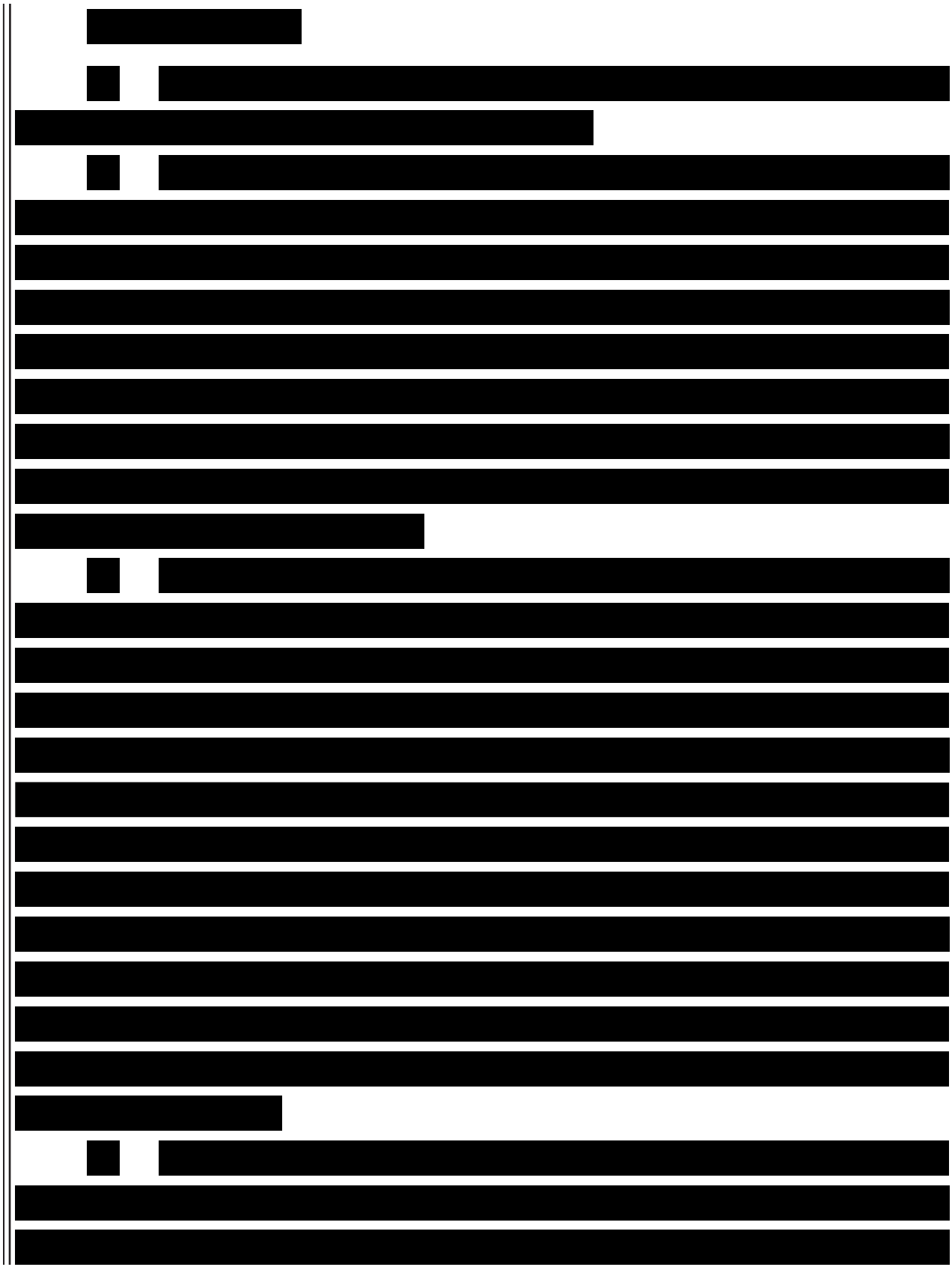
[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

THE SUBJECT USER's ACTIVITY ON THE TARGET WEBSITE

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

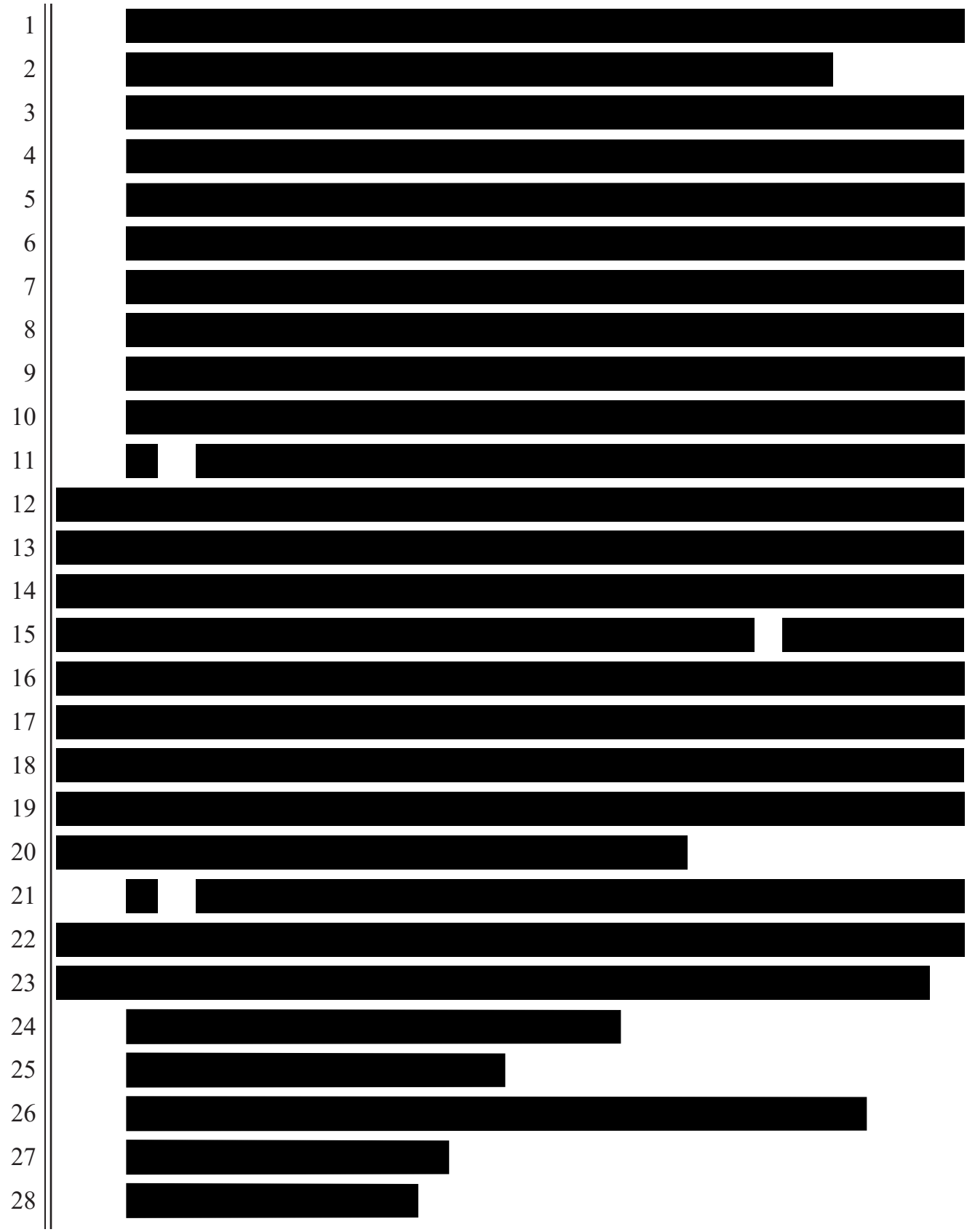


UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

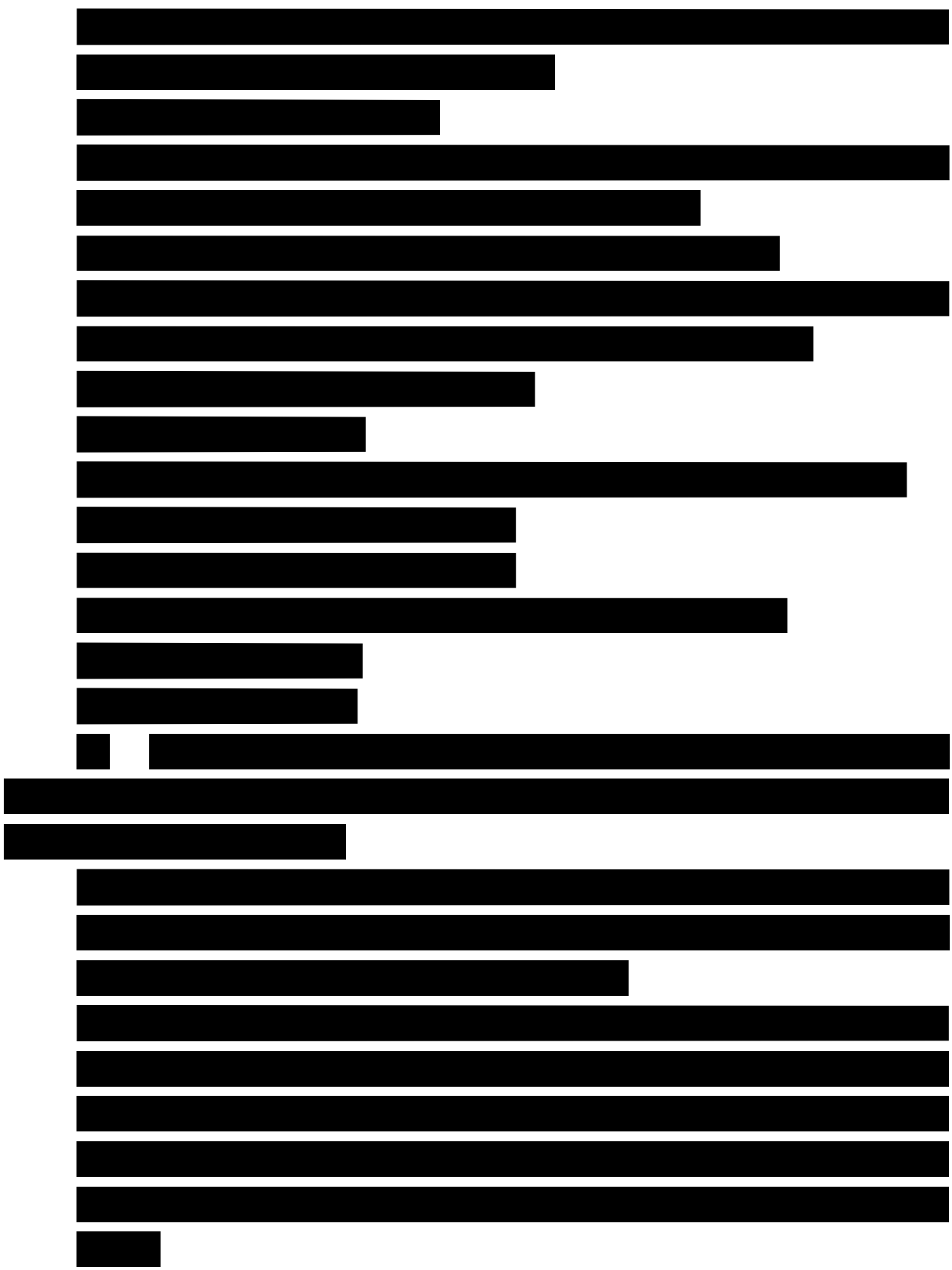
[redacted]

[4] I am aware of the decision in *United States v. Perkins*, 850 F.3d 1109 (9th Cir. 2017). I have consulted with an Assistant United States Attorney and been advised that the United States Attorney's Office for the Western District of Washington does not believe *Perkins* requires review of the imagery described above by the issuing magistrate judge. However, that imagery can be made available for review upon request as part of this application.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



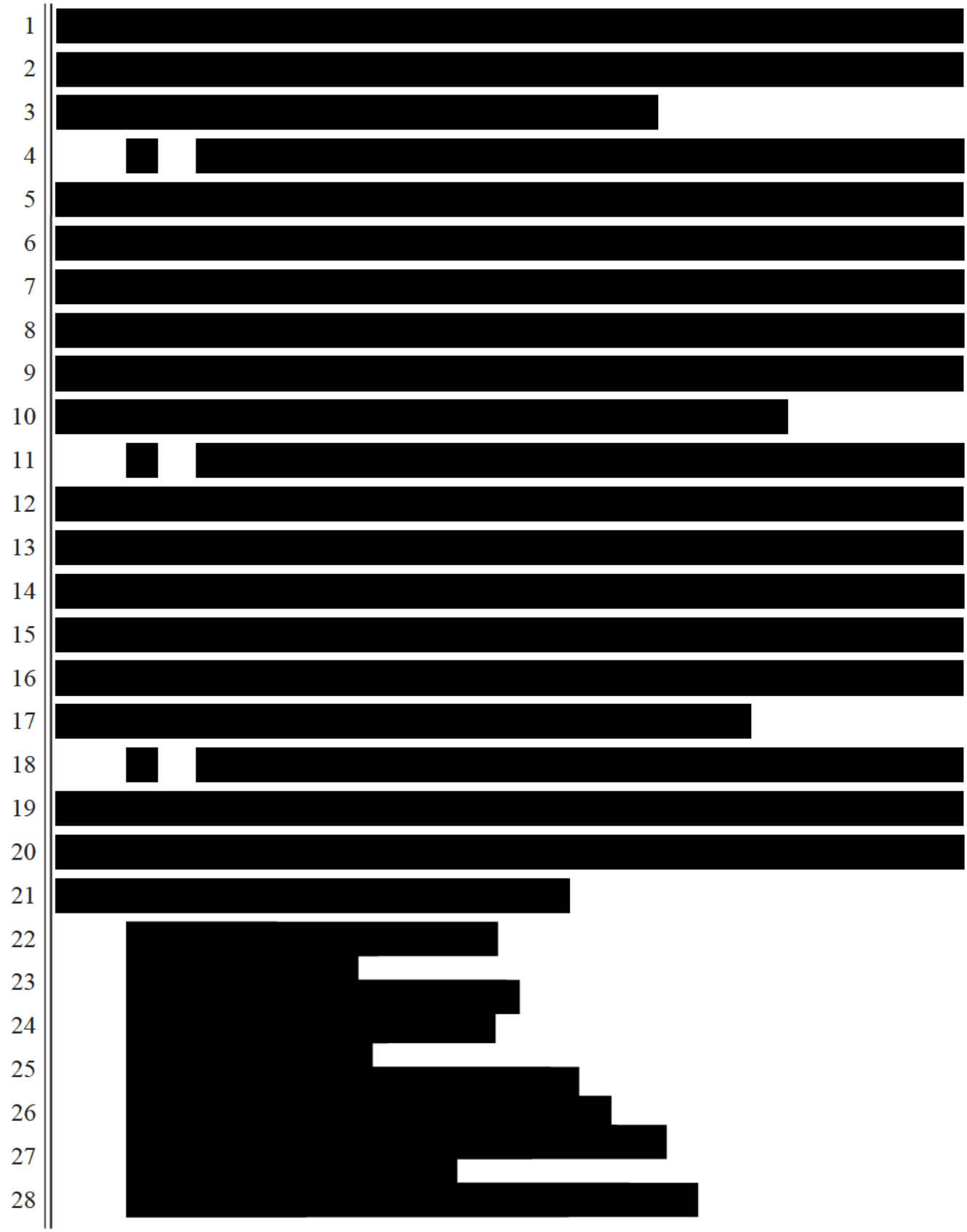
UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

EVIDENCE IDENTIFYING THE SUBJECT PREMISES AND THE SUBJECT USER

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790



UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

53. On or about March 7, 2023, I conducted a phone call to determine the true user of the (564) 654-3752 number. Specifically, I called (564) 654-3752 and asked for "Joe." An adult male answered and stated "this is Joe." After a brief conversation, I stated

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

that I had called the wrong number, apologized, and hung up. Based on this interaction and the other information within this affidavit, I believe it is probable that Joseph Martin is the user of the (564) 654-3752 phone number.

54. A review of publicly available records listed the following possible residents of 310 NE Kissin Tree Lane, Tahuya, Washington 98588:

a. Joseph Martin, year of birth: 1991; and

b. Collin Russell, year of birth: 1993.

55. On or about March 23, 2023, a search warrant was issued by the United States District Court in the Southern District of Florida authorizing the collection of location information related to the cellular phone assigned (564) 654-3752. The FBI received location data from on or about March 28, 2023, through on or about April 26, 2023. A review of that data appeared to show that the user of the cell phone with the number (564) 654-3752 spent nights at the SUBJECT PREMISES and worked on Joint Base McChord/Fort Lewis in Washington.

56. On August 3, 2023, a second search warrant was issued by the United States District Court in the Southern District of Florida authorizing the collection of location information related to the cellular phone assigned (564) 654-3752. A review of location data in response to that warrant indicated that Joseph Martin continues to reside at the SUBJECT PREMISES.

57. The United States Army provided records indicating that Joseph Martin had authorized access to Joint Base McChord/Fort Lewis. The FBI then compared records showing when Joseph Martin accessed the base with the location information related to user of the cell phone assigned number (564) 654-3752. This analysis revealed that on the 18 days between March 28, 2023, through April 26, 2023, when the phone with (564) 654-3752 traveled to the base, Joseph Martin also accessed the base. On the days when Joseph Martin did not access the base, the phone with the number (564) 654-3752 assigned to it did not travel to the base.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

58. Based on the information outlined in this affidavit, I submit that there is probable cause that Joseph Martin is the SUBJECT USER.

59. The FBI conducted aerial surveillance of the SUBJECT PREMISES which disclosed multiple vehicles located on the premises. The rural nature of the SUBJECT PREMISES rendered physical surveillance difficult without potentially alerting the residents.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

60. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

61. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Importantly, e-mail and cloud storage can be a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, and possibly reducing the amount of any evidence of any of that material on the users' computer(s).

[redacted]

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

[redacted]

62. Even if such individuals use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

63. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents, and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

64. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the SUBJECT USER likely has a sexualized interest in children and depictions of children, and that the SUBJECT PREMISES/USER are likely to contain evidence, fruits, and instrumentalities of the TARGET OFFENSES.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

65. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices[5] such as computer hard drives or other electronic storage media.[6] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

66. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found during the search of the SUBJECT PREMISES/USER, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As noted above, I believe the SUBJECT USER has used digital devices and electronic storage media to access the TARGET WEBSITE, a website dedicated to the sexual exploitation of children, where child pornography is exchanged. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities

---

[5] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[6] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

of the TARGET OFFENSES exists and will be found on digital devices or other electronic storage media found in a search of the SUBJECT PREMISES/USER, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

67. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the search of the SUBJECT PREMISES/USER because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[7] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes

[7] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

68. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

69. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

70. Because it is possible that several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

71. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[8]

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

---

[8] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

b. These methodologies, techniques and protocols may include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. OR - Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results.

BIOMETRIC UNLOCK

72. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face, iris, or retina. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. While not as prolific on digital devices as fingerprint and facial-recognition features, both iris and retina scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device, and may not be the only individual whose physical characteristics are among those that will unlock the device via biometric features. Furthermore, while physical proximity is an important factor in determining who is the user of a device, it is only one among many other factors that may exist.

73. Due to the foregoing, I request that if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and if law enforcement reasonably suspects JOSEPH MARTIN is a user of the device, then – for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant – law enforcement personnel shall be authorized to:(1) press or swipe the fingers (including

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

thumbs) JOSEPH MARTIN to the fingerprint scanner of the device; and/or (2) hold the device in front of the face and open eyes of JOSEPH MARTIN and activate the facial, iris, or retina recognition feature.

74. In pressing or swiping an individual's thumb or finger onto a device and in holding a device in front of an individual's face and open eyes, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

CONCLUSION

75. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be found during a search of the SUBJECT PREMISES and the SUBJECT USER if located on the premises, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES and the SUBJECT USER if located on the premises, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

76. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

DAVID BACKLUND

Digitally signed by DAVID BACKLUND
DN: c=US o=U.S. Government ou=Dept of Justice ou=FBI cn=DAVID BACKLUND 0.9.2342.19200300.100.1.1=15001004058341
Date: 2023.08.09 16:41:16 04'00'

DAVID J. BACKLUND
Special Agent

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 11th day of August, 2023.

DAVID W. CHRISTEL
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

ATTACHMENT A

The SUBJECT PREMISES is the property located at **310 NE Kissin Tree Lane, Tahuya, Washington 98588**, containing a two-story residence with an attached, one door garage. The number "310" is displayed prominently on the front of the residence.

Overhead view identifying 310 NE Kissin Tree Lane, Tahuya, Washington 98588

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Photo depicting 310 NE Kissin Tree Lane, Tahuya, Washington 98588, from above

Photo depicting 310 NE Kissin Tree Lane, Tahuya, Washington 98588, from above

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Photo depicting front310 NE Kissin Tree Lane, Tahuya, Washington 98588, from above (photo taken from MLS listing)

The search is to include the residential building, any appurtenances thereto, and any outbuildings, storage units, containers, and vehicles located on the SUBJECT PREMISES, as well as any digital devices or electronic storage media found therein. However, if executing agents can reasonably determine onsite that a particular digital device or electronic storage medium is neither owned nor accessed by the SUBJECT USER, this warrant **DOES NOT** authorize its seizure or search.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The SUBJECT USER is identified as JOSEPH MARTIN, date of birth: XX/XX//1991.

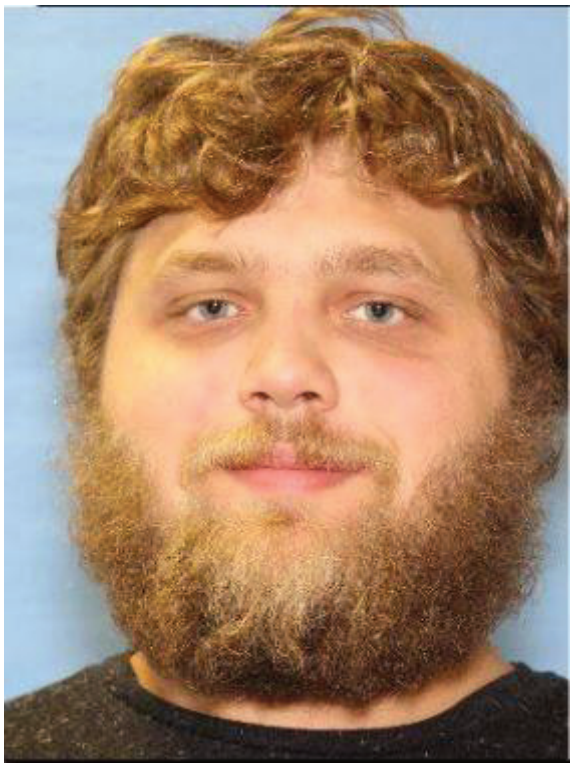


Photo of Joseph Martin

The search is to include the SUBJECT USER and any backpacks, bags, or other containers that the SUBJECT USER may be capable of carrying, as well as any digital devices or electronic storage media found.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252A(a)(1), (a)(2), (a)(5)(B), (b)(1), (b)(2), and (g) (transportation, distribution, receipt, possession, and access with intent to view child pornography, conspiracies and attempts to commit such offenses, and engaging in a child exploitation enterprise) and 18 U.S.C. § 2251(d) and (e) (advertising child pornography and conspiracy and attempt to advertise child pornography) (the TARGET OFFENSES):

1. Documents, records, and things that constitute evidence of who exercises dominion and control over the SUBJECT PREMISES.

2. All records relating to violations of the TARGET OFFENSES, including:

a. visual depictions of minors engaged in sexually explicit conduct

b. identifying information for any individuals shown in such depictions or evidence that would otherwise assist in the identification of those depicted or those responsible for creating such visual depictions

c. information concerning the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct

d. information identifying the source of any visual depictions of minors engaged in sexually explicit conduct

e. evidence of communications related to the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct

f. evidence of contact with or communications about minors

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. evidence indicative of a sexualized interest in minors or depictions of minors

[redacted]

3. Digital devices[9] or other electronic storage media[10] and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

---

[9] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[10] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

5. Records and things evidencing the use of the internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. During the execution of the search of the SUBJECT PREMISES/USER described in Attachment A, if law enforcement encounters a smartphone or other electronic device equipped with a biometric-unlock feature, and if law enforcement reasonably suspects the SUBJECT USER is a user of the device, then – for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant – law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of such person to the fingerprint scanner of the device; and/or (2) hold the device in front of the face and open eyes of such person and activate the facial, iris, or retina recognition feature.

7. In pressing or swiping an individual's thumb or finger onto a device and in holding a device in front of an individual's face and open eyes, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to located evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970